



**F E D E R A L
S T U D E N T A I D**

We Help Put America Through School

FSA Integration Partner

Task Order 144

E-Authentication & E-Signature Support

**E-Authentication (E-Gov)
Project Performance Report
(September – December, 2003)**

Deliverable 144.1.1 – Revised

January 23, 2004

TABLE OF CONTENTS

AMENDMENT HISTORY	2
1 INTRODUCTION & ORGANIZATION OF THE DOCUMENT.....	3
1.1 INTRODUCTION.....	3
1.2 ORGANIZATION OF THE DOCUMENT	3
2 PROJECT WORK PLAN.....	4
3 TASK ORDER ACTIVITIES.....	6
3.1 INTER-AGENCY COMPUTER MATCHING AGREEMENT	7
3.2 FSA-HHS E-SIGN PILOT.....	7
3.3 REVIEW SUPPORT FOR E-GOV E-AUTHENTICATION EMERGING DOCUMENTS.....	7
3.3.1 <i>Guiding Principles</i>	10
3.4 ED PIN CREDENTIAL ASSESSMENT.....	11
3.5 NIH-EDUCAUSE PKI PILOT SUPPORT.....	11
3.6 ADDITIONAL FSA E-AUTHENTICATION OPPORTUNITIES.....	11
4 WHITE PAPER: DEVELOP AN FSA E-AUTHENTICATION, E-ID & E-SIGN BUSINESS PLAN	12
5 REFERENCES	20
5.1 MEETING MINUTES	20
5.2 FSA-HHS E-SIGN (E-GOV E-AUTHENTICATION) PILOT DESCRIPTION	30

Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY
01/22/2004	2	Project Work Plan detail is illustrated.	N. Sattler	Y. Katyal
01/22/2004	4	White Paper is updated with action recommendations.	N. Sattler	Y. Katyal

1 INTRODUCTION & ORGANIZATION OF THE DOCUMENT

1.1 Introduction

The FSA Integration Partner is one of the various groups working with the Office of Applications Development in its implementation of E-Gov E-Authentication initiatives; both internally within FSA as well as externally across agencies. During the 1st quarter of fiscal year 2004 the initiatives supported include the inter-agency computer matching agreement, the FSA-HHS E-Sign Pilot, review support for E-Gov E-Authentication documents, the ED PIN credential assessment activities, NIH-EDUCAUSE PKI pilot participation as well as the identification of additional FSA E-Authentication opportunities.

The purpose of this performance report is to document the FSA Integration Partner activities during the quarter. This report details activities during the current reporting period. A white paper documenting FSA's E-ID, E-Authentication and E-Sign direction is also included as part of this deliverable.

1.2 Organization of the Document

The following sections within this document include:

- Project Work plan
- Task order activities completed during the reporting period
- White Paper on FSA E-Authentication.

Minutes from project meetings are included in the References section at the end of the document.

2 PROJECT WORK PLAN

The current project work plan for activities within the task order is illustrated in the figure on the following page. Initiated in August, 2003, the period of performance for the task order ends on January 30, 2004.

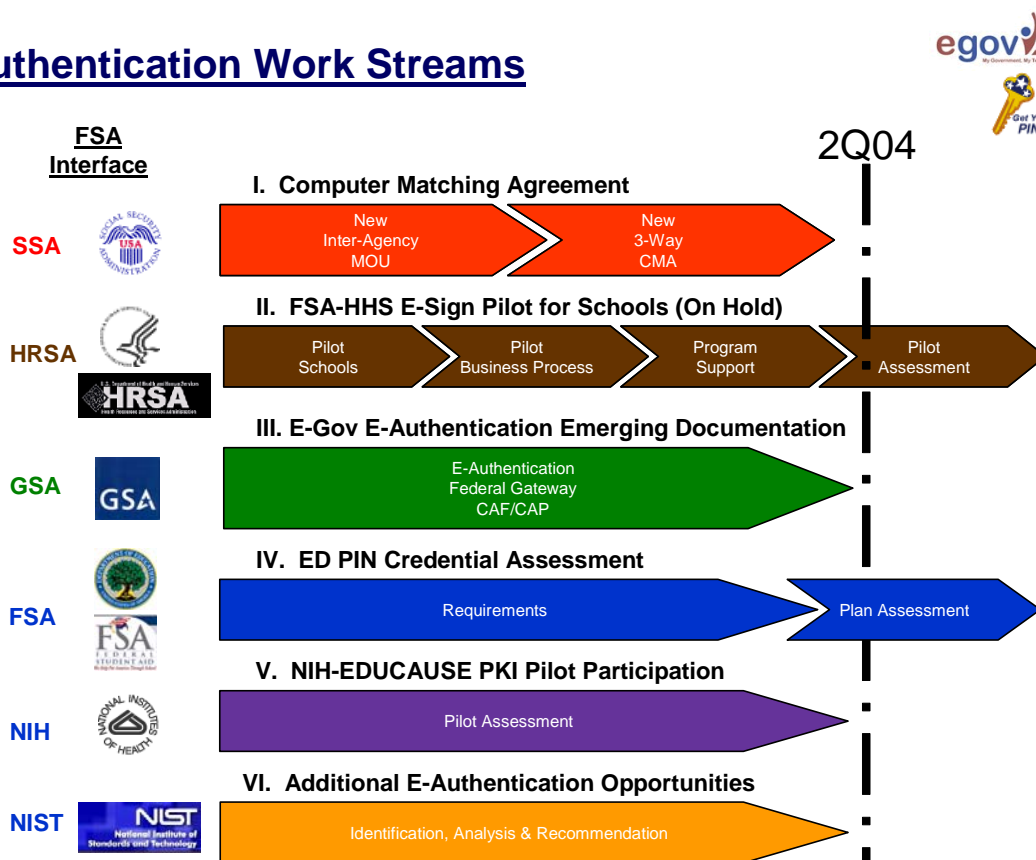
ID	Task Name	Duration	Start	Finish						2004			
					Aug	Sep	Oct	Nov	Dec	Jan	Feb		Mar
1	Task Order 144 Period of Performance	116 days?	Fri 8/22/03	Fri 1/30/04									
2	Award task order	0 days	Fri 8/22/03	Fri 8/22/03	8/22								
3	Kick-off meeting	0 days	Tue 9/2/03	Tue 9/2/03	9/2								
4	Support Activities (incl. bi-weekly status) - Ongoing	102 days	Tue 9/2/03	Thu 1/22/04									
5	Task Order Meeting	0 days	Tue 9/2/03	Tue 9/2/03	9/2								
6	Task Order Meeting	0 days	Thu 9/4/03	Thu 9/4/03	9/4								
7	Task Order Meeting	0 days	Mon 9/8/03	Mon 9/8/03	9/8								
8	Task Order Meeting	0 days	Thu 9/11/03	Thu 9/11/03	9/11								
9	Task Order Meeting	0 days	Mon 9/22/03	Mon 9/22/03	9/22								
10	Task Order Meeting	0 days	Thu 9/25/03	Thu 9/25/03	9/25								
11	Task Order Meeting	0 days	Mon 9/29/03	Mon 9/29/03	9/29								
12	Task Order Meeting	0 days	Thu 10/2/03	Thu 10/2/03	10/2								
13	Task Order Meeting	0 days	Thu 10/9/03	Thu 10/9/03	10/9								
14	Task Order Meeting	0 days	Thu 10/16/03	Thu 10/16/03	10/16								
15	Task Order Meeting	0 days	Wed 10/29/03	Wed 10/29/03	10/29								
16	Task Order Meeting	0 days	Thu 11/13/03	Thu 11/13/03	11/13								
17	Task Order Meeting	0 days	Thu 12/4/03	Thu 12/4/03	12/4								
18	Task Order Meeting	0 days	Thu 12/18/03	Thu 12/18/03	12/18								
19	Task Order Meeting	0 days	Thu 1/8/04	Thu 1/8/04	1/8								
20	Task Order Meeting	0 days	Thu 1/15/04	Thu 1/15/04	1/15								
21	Task Order Meeting	0 days	Thu 1/22/04	Thu 1/22/04	1/22								
22	Task Order Meeting	0 days	Thu 1/29/04	Thu 1/29/04	1/29								
23	PKI Pilot Meeting	0 days	Thu 10/2/03	Thu 10/2/03	10/2								
24	Technology Meetings - Ongoing (As Required)	47 days	Thu 9/25/03	Fri 11/28/03									
25	Policy Meeting	0 days	Mon 9/8/03	Mon 9/8/03	9/8								
26	Credential Assessment Initial Meeting	0 days	Tue 9/30/03	Tue 9/30/03	9/30								
27	Meetings with WebCAAF re: credential assessment framework	23 days	Mon 9/15/03	Wed 10/15/03									
28	ED PIN Re-Engineering Review	24 days	Mon 9/15/03	Thu 10/16/03									
29	8th Federal Education PKI Meeting	0 days	Tue 12/16/03	Tue 12/16/03									
30	Task Order Modification	34 days	Mon 11/24/03	Thu 1/8/04									
31	144.1.1 E-Authentication (E-Gov) Project Performance Report	20 days	Thu 12/4/03	Wed 12/31/03									
32	Submit Deliverable 144.1.1 to FSA	0 days	Wed 12/31/03	Wed 12/31/03									
33	FSA Feedback on Deliverable	0 days	Thu 1/15/04	Thu 1/15/04									
34	Revise Deliverable per FSA Feedback	6 days	Thu 1/15/04	Thu 1/22/04									
35	Add detail to project plan	6 days	Thu 1/15/04	Thu 1/22/04									
36	Add detail to recommendations in White Paper	6 days	Thu 1/15/04	Thu 1/22/04									
37	Resubmit Deliverable 144.1.1	0 days	Thu 1/22/04	Thu 1/22/04									
38	1. Comments on Emerging Documents	14 days	Mon 11/17/03	Thu 12/4/03									
39	NIST 800-63 Draft Recommendation for Electronic Authentic	7 days	Mon 11/17/03	Tue 11/25/03									
40	Review Documentation	7 days	Mon 11/17/03	Tue 11/25/03									
41	Comments provided to FSA	0 days	Tue 11/25/03	Tue 11/25/03									
42	E-Authentication Strategic Business Plan - DRAFT	8 days	Tue 11/25/03	Thu 12/4/03									
43	Review Documentation	8 days	Tue 11/25/03	Thu 12/4/03									
44	Comments provided to FSA	0 days	Thu 12/4/03	Thu 12/4/03									
45	2. FSA Computer Matching Agreement (FSA)	104 days	Fri 9/5/03	Wed 1/28/04									
46	Support FSA tasks for CMA approval	102 days	Fri 9/5/03	Mon 1/26/04									
47	Help understand approval process	10 days	Thu 1/15/04	Wed 1/28/04									
48	Receive process documentation from FSA	0 days	Fri 1/16/04	Fri 1/16/04									
49	Discuss process with Marya Dennis, FSA	0 days	Fri 1/23/04	Fri 1/23/04									
50	Work with FSA to Summarize Actions/Next Steps	2 days	Fri 1/23/04	Mon 1/26/04									
51	CMA Process Summary	0 days	Mon 1/26/04	Mon 1/26/04									
52	3. White Paper - FSA E-Authentication Position	41 days	Thu 12/4/03	Fri 1/30/04									
53	Prepare initial draft	20 days	Thu 12/4/03	Wed 12/31/03									
54	Update white paper	20 days	Fri 1/2/04	Thu 1/29/04									
55	Submit with Deliverable 144.1.2	0 days	Fri 1/30/04	Fri 1/30/04									
56	4. Credential Assessment Framework Support for ED PIN	88 days	Tue 9/30/03	Thu 1/29/04									
57	Support FSA activities	85 days	Tue 9/30/03	Mon 1/26/04									
58	Propose high level tasks/objectives	0 days	Mon 1/19/04	Mon 1/19/04									
59	Support FSA activities with assessment planning	8 days	Tue 1/20/04	Thu 1/29/04									
60	5. FSA-HHS E-Sign Pilot for Schools	85 days	Tue 9/30/03	Mon 1/26/04									
61	Support process	85 days	Tue 9/30/03	Mon 1/26/04									
62	6. EDUCAUSE/NIH/Higher Education Pilot Support	85 days	Wed 10/1/03	Tue 1/27/04									
63	Support activities	85 days	Wed 10/1/03	Tue 1/27/04									
64	Document high level summary	0 days	Mon 10/6/03	Mon 10/6/03									
65	144.1.2 E-Gov E-Authentication Opportunities Support	21 days?	Fri 1/2/04	Fri 1/30/04									
66	Update White Paper	21 days?	Fri 1/2/04	Fri 1/30/04									
67	Document CMA Approval Process	6 days?	Fri 1/16/04	Fri 1/23/04									
68	Work with Marya Dennis/FSA	6 days?	Fri 1/16/04	Fri 1/23/04									
69	Receive process documentation	0 days	Fri 1/16/04	Fri 1/16/04									
70	Meeting with Marya Dennis	0 days	Fri 1/23/04	Fri 1/23/04									
71	Summarize process	0 days	Fri 1/23/04	Fri 1/23/04									
72	Help Review CAF Material	6 days?	Fri 1/16/04	Fri 1/23/04									
73	Meeting with Schools, Data Strategy, etc.	10 days?	Mon 1/19/04	Fri 1/30/04									
74	Prepare Deliverable 144.1.2	5 days?	Mon 1/26/04	Fri 1/30/04									
75	Submit Deliverable 144.1.2 to FSA	0 days	Fri 1/30/04	Fri 1/30/04									
76	Future Considerations for FSA	2 days	Mon 2/9/04	Tue 2/10/04									
77	NIST Knowledge Based Authentication Symposium	2 days	Mon 2/9/04	Tue 2/10/04									

3 TASK ORDER ACTIVITIES

This section documents the 6 areas of FSA Integration Partner support within this task order. The level of FSA Integration Partner support across these areas varies and is documented accordingly. The specific level of support is noted below in the individual discussion. The areas include:

- Inter-Agency Computer Matching Agreement
- FSA-HHS E-Sign Pilot
- Review Support for E-Gov E-Authentication Emerging Documents
- ED PIN Credential Assessment
- NIH-EDUCAUSE PKI Pilot Participation
- Additional FSA E-Authentication Opportunities

E-Authentication Work Streams



An illustration of the 6 “work streams” is shown above. A description of each support activity is provided in the following subsections.

3.1 Inter-Agency Computer Matching Agreement

FSA Integration Partner support for the review and establishment of an inter-agency computer matching agreement (CMA) has been minimal. FSA's Office of Applications Development has planned and completed this activity which will allow the agency to extend the ED PIN as an authentication and E-Sign credential to other agencies for conducting web transactions with the student community. FSA has primarily worked with the U.S. Department of Education (ED), U.S. Department of Health and Human Services (DHHS), U.S. Social Security Administration (SSA), and Office of Management and Budget (OMB) to achieve this significant milestone.

3.2 FSA-HHS E-Sign Pilot

FSA Integration Partner support for the FSA-HHS E-Sign Pilot has included project management and technical advisory services. FSA's Office of Applications Development has planned and managed this effort including the necessary interfaces with DHHS, the U.S. General Services Administration (GSA), OMB, pilot schools and contractors. This pilot is currently on hold pending forthcoming E-Authentication guidance from GSA. This project was placed on hold when GSA decided to revise the E-Authentication Gateway infrastructure. The FSA-HHS E-Sign Pilot design included the use of the E-Authentication Gateway - the gateway was closed to new projects effective October 10, 2003. New guidance from GSA is expected during the 2nd quarter of the fiscal year at which point the FSA-HHS pilot design will be updated accordingly. The pilot will be re-evaluated at that time to determine future direction and tasks.

3.3 Review Support for E-Gov E-Authentication Emerging Documents

FSA Integration Partner review support included the following emerging documents:

- Draft - E-Authentication Credential Assessment Framework
- Draft - E-Authentication Common Credential Assessment Profile
- Draft - E-Authentication PIN Credential Assessment Profile
- Draft - E-Authentication Strategic Business Plan
- Draft - E-Authentication Interface Specifications for the SAML Artifact Profile
- Draft - NIST Special Publication 800-63, Recommendation for Electronic Authentication
- Other

A summary of the key elements of the review support is documented below.

A (credential assessment) framework is clearly necessary to foster the right level of trust for inter-agency use of electronic credentials issued to individuals by a U.S. Government agency.

Suggestions included:

1. Focus efforts on a credential framework rather than assessment criteria. Development of credential models will help provide guidance for different types of credentials. The different types of credentials may be linked to OMB guidance on levels of authentication. The credential framework can then be used across Government agencies and can be facilitated through an E-Authentication Service (e.g., gateway and/or other facilities).
2. Leverage existing standards and involve industry groups. NIST, ISO, IEEE, Liberty Alliance, Meteor, and various other organizations have identification and authentication standards that should be leveraged where appropriate to avoid “reinventing standards” (e.g., FIPS PUB 112 <http://www.itl.nist.gov/fipspubs/fip112.htm>).
3. Solicit industry expertise (as part of steering committee or action team) for development of credential framework.
4. Requirements that can not be measured should be avoided. For example, staffing, subcontracts, identity proofing records, etc. In some instances, documentation related to the requirements will not be shared for any assessment with any contractor – e.g., data center security records.
5. Business needs of credentials issued should be taken into consideration as part of the profile or framework and addressed separately from technical specifications. For example, version control for software components.
6. May want to consider sensitivity to certain terms. For example, “organizational maturity” has little to do with credential integrity and strength; e.g., the U.S. Department of Homeland Security is “immature” per these criteria.
7. The team may want to consider addition of some criteria for knowledge-based credentials, e.g., SSN.
8. The team may want to consider addition of criteria for continuous maintenance of credential integrity.
9. Related to the PIN CAF, it was unclear whether this profile is associated with credentials that include issuance of a user ID or not.
10. GSA should interface with the Federal organization responsible for standards – NIST.

High Level Review Comments – NIST Special Publication 800-63, DRAFT Recommendation for Electronic Authentication.

The draft addresses several factors related to authentication of individual people over an open network: the registration process (claimant, verifier, establishing an identity, and relying parties), tokens (e.g., password, cryptographic key, smart card, voice print, biometrics), verifiers and assertions (e.g., SAML, cookies, etc.). The draft also illustrates how electronic authentication can vary relative to the strength of a credential itself (i.e., difficulty of guessing, forging, or otherwise compromising a credential) and discusses the potential use of entropy to determine requisite strength of a credential/password.

The ED PIN as an authentication credential. It is not simply a PIN password or PIN number. The ED PIN credential is the US Department of Education, FSA name for the credential that includes a person’s social security number, date of birth, first two letters of the last name, and a 4-digit password. The first three components of the ED PIN credential are knowledge-based aspects related to an individual. The paper does not consider knowledge-based authentication methods. The draft indicates that guidance for knowledge-based authentication will be made available but no timeframe is provided. The analysis

of knowledge-based authentication using other models would not do proper justice to the ED PIN credential strength.

The current ED PIN possesses important controls that need to be recognized. For example: SSL/TLS protects the channel and prevents eavesdropping; the ED PIN is encrypted during storage; accounts are locked after a specified number of incorrect login attempts, which increases the difficulty of guessing the credential. There are other controls as well.

One suggestion would be for FSA to partner with NIST, and/or GSA (as appropriate), to help develop the knowledge-based authentication framework. Other federal agencies interested in this framework may also be included in this effort.

Comments on the E-Authentication Strategic Business Plan included the following:

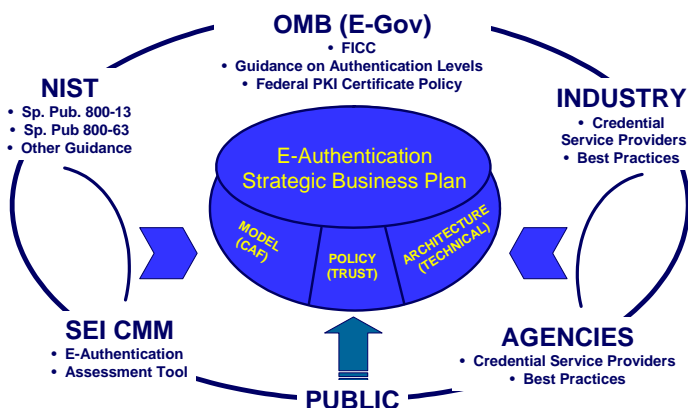
General:

1. The Plan has identified many of the relevant issues, milestones, performance measures and risks that need to be addressed to “make trust possible”.
2. The Plan is weak in the knowledge-based method of authentication used heavily in FSA (and SSA). Our “PIN Plus” authentication approach is not addressed in this Plan.
3. The interim E-Authentication architecture specifics not defined at all in this Plan. We know this is a difficult task to do and that specifics are being developed but specifics are needed in the Plan.
4. This document should build upon the NIST (800-13 Draft Recommendation for E-Authentication) and the SEI risk-based approach to authentication requirements deliverable (E-Authentication Risk and Requirements Analysis) rather than develop its own similar guidance. The E-Authentication Policy Framework graphic (Page 13) should be re-drawn to better represent how various “drivers” influence the policy. See suggested revised framework that is attached.
5. The Plan does not adequately define *how* the “Circle of Trust” and “Transitive Trust” concepts will be approached. This area is not well described and too high level.

Specific:

1. Industry involvement should occur earlier in the timeline. This would leverage available existing services better. (Page 24)
2. The Technical Approach chapter (Page 14-16) is neither technical nor specific.

Included in the comments was the illustration shown below:



3.3.1 Guiding Principles

The guiding principles for reviewing emerging guidance centers around the following:

- A. Any compromise to the current strength and business use related to the ED PIN is not an option.
- B. The ED PIN credential uses knowledge-based authentication for both authentication and electronic signature, i.e., no user ID is issued. This model works for FSA and its student customers and a framework supporting knowledge-based authentication should be developed.
- C. FSA is open to guidance that will provide additional alternatives for authentication and electronic signatures in addition to the ED PIN.

To-date, the Office of Applications Development has been able to provide valuable feedback in the form of experience as well as standards review to the various groups pursuing additional E-Authentication guidance.

3.4 ED PIN Credential Assessment

The FSA Integration Partner support for the ED PIN credential assessment has been limited to framework and document review. While initially planned for the 1st quarter of the fiscal year, this assessment is currently delayed until the credential assessment framework is more fully developed to handle the ED PIN requirements.

3.5 NIH-EDUCAUSE PKI Pilot Support

The FSA Integration Partner support for the NIH-EDUCAUSE PKI pilot has included attendance at technical meetings as well as the 8th Federal PKI meeting in December. Working with the FSA Office of Applications Development, the participation in this pilot is focused on examining the success of PKI technology used by NIH and EDUCAUSE at 6 pilot schools¹ to electronically sign XML forms. The pilot has demonstrated considerable promise for business functions at FSA; especially, with trading partners. FSA is currently assessing the pilot's success and applicability to specific FSA business processes.

3.6 Additional FSA E-Authentication Opportunities

FSA Integration Partner activities in identifying additional FSA E-Authentication opportunities are still ongoing. The 2 areas being researched for opportunities include:

- Case Management and Oversight (CMO), and
- Trading Partner Management (TPM).

The business processes supporting CMO help FSA mitigate risk of fraud as well as compliance issues associated with Title IV fund disbursements. Risks are continuously evolving and the CMO function helps increase level of compliance through the application (system) indicators, FISAP-related indicators, non-submission of required reporting (e.g., FISAP, SSCR, IPEDS, recertification, etc.), funding-related indicators, program administration-related indicators, early warnings and other data analysis approaches.

The TPM initiative addresses the business functions associated with higher education institutions, financial partners (lending organizations, guarantee organizations, etc.) and other non-student communities. Numerous processes support the TPM life cycle functions requiring interface with FSA and the U.S. Department of Education and may offer additional E-Authentication opportunities. An initial recommendation of opportunities in both the CMO and TPM arena is currently planned during the 2nd quarter of the fiscal year.

¹ The 6 pilot schools include – University of California (Berkley), University of Texas – Health Sciences Center, Dartmouth College, University of Virginia, University of Wisconsin (Madison) and University of Alabama.

4 WHITE PAPER: Develop an FSA E-Authentication, E-ID & E-Sign Business Plan

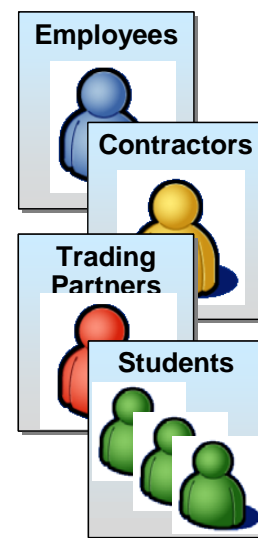
Purpose

The purpose of this White Paper is to communicate the need for an FSA enterprise-wide business plan to structure, strengthen and expand FSA leadership in E-ID, E-Authentication and E-Sign initiatives. The White Paper suggests specific actions that should be undertaken to continue an enterprise focus across multiple E-ID related initiatives. This White Paper discusses FSA Expertise, the Current Landscape, Anticipated Growth, Technical Infrastructure, Business Considerations and Opportunities. The specific actions suggested include near term, medium term and long term implementation opportunities.

Seven years of experience with the knowledge-based ED PIN credential now suggests the need for limiting it to Student use and examining other options for Trading Partners. A business plan is necessary to strengthen the current credential and associated technologies while introducing or examining other credential(s). Any change will need to be accomplished without disruption to current service.

FSA will Need Expertise Beyond the ED PIN to sustain E-ID, E-Authentication & E-Sign Leadership

The CIO Office of Applications Development at the U.S. Department of Education (ED) Office of Federal Student Aid (FSA) has been at the forefront promoting *E-Authentication* as a key strategy for enabling e-Gov business goals. Having successfully developed and promoted the business case related to *E-Sign* (electronic signatures) for FSA customers, the Office of Applications Development implemented E-Sign for promissory notes in the Direct Loan, FFEL and Perkins programs as well as the FAFSA. The Free Application for Federal Student Aid (FAFSA) offers, since 1997, a completely paperless process to over 6 million annual applicants seeking financial aid. The catalyst for achieving rapid success has been the Office of Applications Development persistent and constant communication with its customers as well as business process owners to understand *E-ID* (electronic credential) requirements. Customer groups include students and trading partners (schools and financial partners – lenders, guarantee agencies, servicers, etc.). Business process owners span all FSA and certain external agencies (e.g., U.S. General Services Administration (GSA), Office of Management and Budget (OMB), E-Gov Initiatives, etc.). The FSA business process owners specifically include the Schools, Financial Partners and Students channels as well as the Office of General Counsel, Policy Development Division, and other support organizations. With over 2 Million E-Sign transactions a year and a user base of over 40 Million, FSA's progress is maturing to the next level. At this level, there is higher need for ensuring security, privacy and confidentiality associated with electronic transactions.



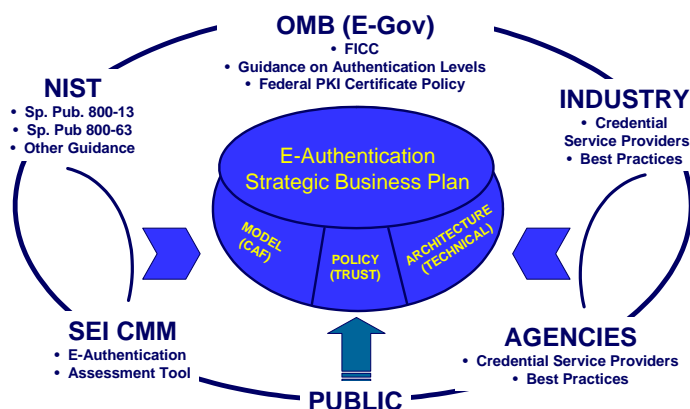
FSA is, and continues to be, sensitive to the security, privacy and confidentiality needs of communities it serves. Paperless alternatives are provided only as options to traditional processes; or as the only option, with agreement from the community. The security certification and accreditation process for its

IT systems includes a focus on security, privacy and confidentiality. This focus will help FSA maintain its leadership position as long as weaknesses related to electronic credentials are documented and adequately removed.

The IT systems at FSA are used by many groups including employees, contractors, trading partners, students, and others. While the ED PIN processes have been successful for E-ID, E-Authentication and E-Sign, there are currently few limitations regarding its applicability for a specific group(s). There are also 40 other authentication processes at FSA in addition to the ED PIN. The business, operational, technical, legal and political needs for an enterprise-wide Business Plan that provides guidance for managing electronic identity is very much necessary. Without such guidance there is a risk of contaminating the integrity associated with the ED PIN (and the over 40 other credentials) that will ultimately counter FSA's E-ID, E-Authentication and E-Sign success.

FSA can Learn from, & Contribute towards, multiple Federal & Industry Initiatives

Significant investment in E-ID-related projects is being made by Federal organizations including OMB, NIST, and other agencies such as FSA, USDA, GSA, NIH, DHHS, etc. Industry attention from numerous organizations, credential service providers and standards groups as well as the Software Engineering Institute (SEI) is also focused on addressing E-ID, E-Authentication and E-Sign needs. Efforts resulting from Federal guidance, combined with industry standards such as the Liberty Alliance and FSA's own business experience are bound to yield best practices that will benefit many organizations including FSA. Not only will a business plan provide structure and direction, but it can also allow FSA with an opportunity to influence some of the emerging architectures, standards and technologies through its first-hand experience.

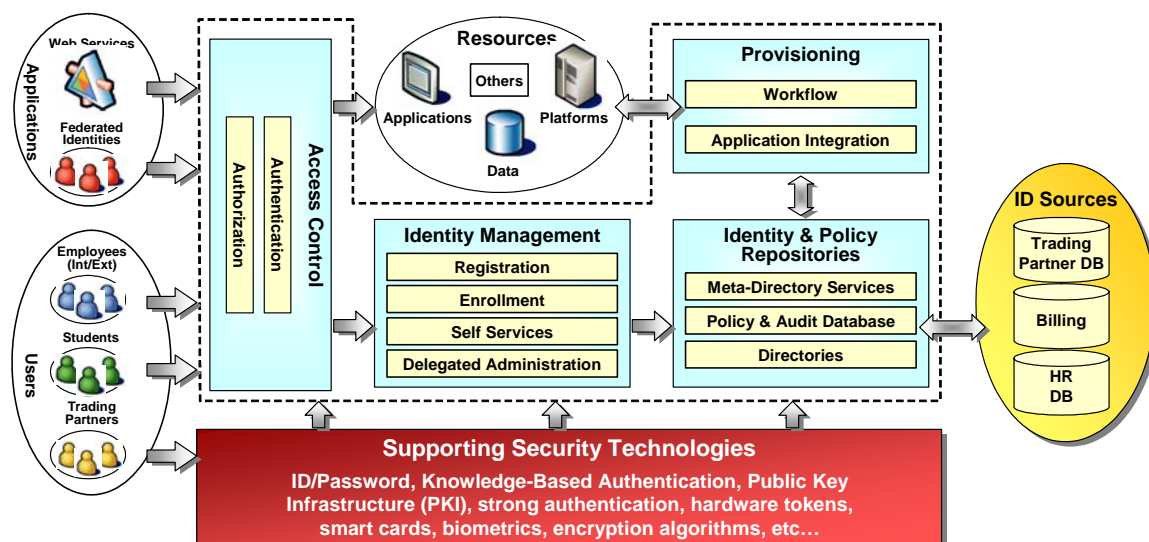


No Turning Back – More Transactions will use the ED PIN With over 6 Million new customers annually, the Opportunity Pipeline for FSA is remarkably rich. These new customers also provide incremental opportunities for electronic service during the financial aid life cycle – expecting to top 100 Million potential users by 2009². Less than 5% of this user base currently takes advantage of E-ID, E-Authentication and E-Sign services. A very significant part of the responsibility for increasing market penetration lies with FSA and its ability to design a sound infrastructure that can continue to service customers while acquiring additional customers at increasing rates. While benefiting customers, these opportunities also provide FSA with the means to service more customers electronically and faster, using industry standards that cost less to integrate and operate, and provide levels of fraud detection and prevention capabilities that are impossible without an enterprise-wide identity management and authentication approach.

² Source: U.S. Department of Education - <http://www.ed.gov/offices/OUS/StudentLoanTables/index.html>

FSA needs to Reduce the number of Customer Credentials

Most of the components for establishing an E-ID, E-Authentication and E-Sign business plan already exist at FSA, albeit duplicative. These include the Identity Management, Provisioning, Repository, Access Control and Interface functions used to manage, issue, store, and utilize the 40+ FSA customer credentials to enable electronic transactions. Most FSA IT systems are electronically accessible (i.e., authentication), possess strong policies and rules for access control (i.e., authorization), comply with standards for system interfaces (i.e., application program interface - APIs, enterprise application integration - EAI connectors, web services, etc.), and provide customer support (i.e., help desk, web chat, etc.). Authentication is also one of the criteria for compliance with security certification and accreditation. FSA also has initiatives to link customer data and provide Single Sign-On³ capability to ease the burden on customers. The focus on all these aspects of infrastructure is yet another reason for developing a business plan to understand the enterprise needs and guide future efforts. One such target enterprise-wide E-ID, E-Authentication and E-Sign architecture is illustrated below.



It is not the intent of this White Paper to recommend any architecture for FSA but simply to identify the need for a business plan containing elements identified above. As such, at this time the architecture above is for illustrative purposes only. The target vision should include E-ID as an objective.

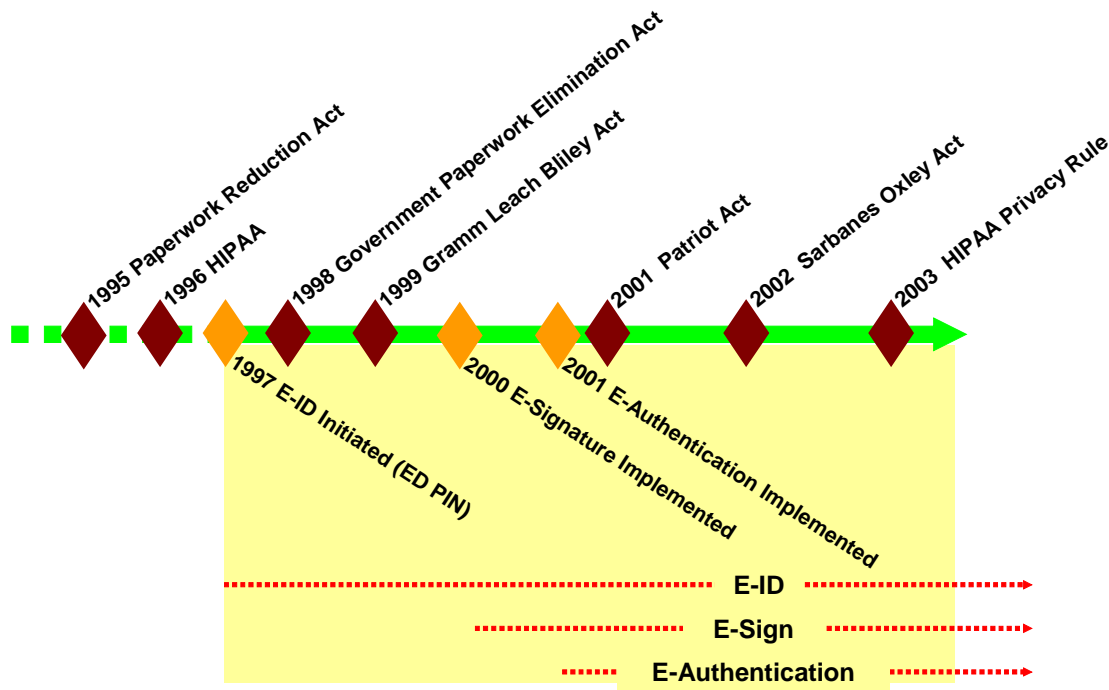
Knowledge-Based Authentication is Important to FSA

Any E-ID, E-Authentication and E-Sign business plan is likely to be unique to an organization. For example at FSA, there are opportunities to design solutions that can support at least 2 different types of customers – students and trading partners. The ED PIN is an excellent implementation for the student community and can be further strengthened using knowledge-based authentication and data management principles. Transitive trust approaches appear to be strong options for trading partner authentication. Transitive Trust Domains can allow flow of attributes to domains that trust them. Regardless, there are many methods that FSA should consider as part of developing an enterprise-wide authentication business strategy. Considerable federal and industry attention to identity management and authentication will

³ One alternative should also include Reduced (as opposed to Single) Sign-On.

also provide guidance on what and how FSA should approach the development of a strategy that includes these considerations (e.g., PKI and other strong authentication alternatives).

Other than technology, the development of a strategic E-ID, E-Authentication and E-Sign business plan will also need to address legislation. FSA has no issue in complying with legislation related to E-Sign or E-Authentication processes. Initial efforts related to paperwork reduction and paperwork elimination legislation are now focused on privacy and security. The three work streams – E-ID, E-Authentication and E-Sign – help FSA focus on compliance activities easily.



Legal aspects, in addition to business issues and technological advances, will also need to be part of the broader guidance. Legislation focusing on privacy and accountability issues includes CPNI, HIPAA, Patriot Act, Gramm Leach Bliley, and Sarbanes-Oxley. Each addresses a particular impact area and has corresponding costs associated with its violation. The following table summarizes these legislative impacts.

Legislation	Impact Area	Violation Cost
Customer Proprietary Network Information (CPNI)	Privacy – Establishes criteria and restrictions for sharing customer information	No precedents have yet been set for violations. Punitive damages in the amount of potential revenue from the violation are plausible.
Health Insurance Portability and Accountability Act (HIPAA)	Privacy and Security – Establishes standard for transaction and information handling to ensure the security and privacy of personal information	Civil penalties: \$100 per violation to \$25,000 per person; Criminal penalties: limited to \$250,000 and a 10 year prison sentence
Patriot Act	Audit and Reporting – Establishes guidelines for enacting anti money-laundering programs and reporting	Civil penalties: up to \$275,000 per violation; Criminal penalties: \$1 million and a 12 year prison sentence

Legislation	Impact Area	Violation Cost
	transactions	
Gramm Leach Bliley	Privacy – Establishes administrative processes as a requirement for broadening activities that financial institutions can partake	Civil penalties: up to \$100,000 per violation; Criminal penalties: \$100,000 and a 5 years in prison sentence
Sarbanes-Oxley	Audit and Reporting – Improve transparency through record retention and reporting of financially relevant information	Criminal penalties: various punishments up to \$25 million fines and 25 years in prison

While Government agencies such as FSA are not directly affected by such legislation, compliance is still good practice.

FSA needs to Strengthen its E-ID Management Plan with Governance, Controls & Partnership

Clearly a leader in E-ID, E-Authentication, and E-Sign, FSA needs to continue to strengthen and increase current service, design new options and contribute to similar industry and federal efforts. The success of FSA's future E-ID efforts will depend on the following:

- Establishment of enterprise-wide E-ID Governance
- Implementation of Management and internal Controls
- Assessment of Alternatives in Cooperation with Customers and Federal/Industry Partners.

An explanation of each opportunity is provided below.

I. GOVERNANCE - Establish enterprise-wide E-ID Governance

FSA's most known E-ID credential is the ED PIN. There are also dozens of other E-ID credentials used within FSA. Most of the other credentials are specific to business applications. There is also no segmentation of credentials based on customers or types of transactions. Furthermore, there is no central responsibility for issuance and management of E-ID credentials. With over 40 credentials being issued and managed concurrently, it is time for FSA to provide enterprise guidance and, more importantly, have the ability to monitor FSA E-ID efforts from an enterprise perspective. Failure to govern this capability will likely result in incompatible, non-standard customer identification schemes that are difficult to integrate and increasingly expensive to maintain. The specific responsibility, and outcomes, for the E-ID governance should include:

1. E-ID Architecture. The purpose of the architecture should be to communicate the vision to optimize number of credential solutions used within the FSA enterprise.
2. Standards. Another aspect of Governance should include the analysis and publication of accepted standards for deploying and implementing credentials regardless of application system, i.e., enterprise-wide.
3. Governance Process. A process should be established, implemented and used enterprise-wide for managing electronic identity and its application within systems. This process should include technical, administrative, investment, and monitoring oversight across all credentials used within FSA.

This governance body must have sponsorship and participation from the Department of Education to be effective.

II. CONTROLS - Implement Management Controls

The number of ED PIN credentials issued by FSA are projected to exceed 90 million by the end of this decade. Lack of management controls will likely compromise this credential. Any compromise of integrity associated with this credential, whether by FSA or one of its customers, will likely force an expensive data clean-up effort. The same controls should be implemented for all FSA credentials. Aspects for consideration include:

4. System Reports. System reports should be reviewed that highlight usage – who is using credentials through which applications, errors, changes, problems, security vulnerabilities, potential fraudulent activity, etc.
5. Internal Controls. The development of management controls should also proactively address potential risks and controls to mitigate those risks. An area relevant to E-ID is identity theft and fraudulent use of credentials. Others will need to be analyzed by FSA as part of this process.
6. Customer Strategy. As part of this process, FSA needs to establish appropriate credentials based on customer group. Alternatively, FSA may want to formally decide to use the ED PIN for various types of identification and authentication purposes by many different customer groups and mitigate against that risk. Either way, a decision from the enterprise perspective is warranted.

III. PARTNERSHIP - Assessment of Alternatives in Cooperation with Customers & Federal/Industry Partners

Preparedness is key. Opportunities exist for FSA to focus its enterprise authentication strategy with a two-pronged perspective. One addressing needs of the large and expanding student community and the other for higher education institutions, financial institutions, states, etc. (trading partners). The student community (i.e., individuals) will likely continue with knowledge-based authentication (ED PIN is an example). FSA will need to support other alternatives for its organizational partners. PKI is one of those alternatives and FSA has an opportunity to “learn and assess” the technological implications to its business processes. A potential large role for PKI looms in organizations requiring strong authentication, electronic signature, data integrity and confidentiality as well as non-repudiation capabilities. Perhaps PKI will mature as its own X.509 implementation or as part of a Web Services framework integrated with operating systems. Successful PKI projects have always been conducted as a partnership of IT and business. FSA has an opportunity to organize an IT/business team to “learn and assess” the PKI technology with a NIH-funded EDUCAUSE proof-of-concept involving FSA customers⁴. This participation will require an organized IT/business partnership and the identification of one FSA form.

⁴ FSA customers include: University of California (Berkley), University of Texas – Health Sciences Center, Dartmouth College, University of Virginia, University of Wisconsin (Madison) and University of Alabama.

The NIH-EDUCAUSE PKI pilot is one of many opportunities that FSA has for examining the business relevance of PKI technology. This pilot is of particular significance since higher education institutions are piloting electronic signature using PKI with XML forms. While many Federal agencies offer PKI capability, FSA does not possess the capability.

PKI is expensive to implement. It is a very sophisticated and complicated technology to plan for, procure, implement, and manage. Participating in a proof-of-concept with others who are learning is the best way to learn the business implications of this technology. It is unlikely FSA will deploy PKI applications for its customers over the next two years. To be prepared, FSA should consider:

7. Risk Assessments. The purpose of risk assessments, especially from 3rd party organizations, helps establish credibility and identify weaknesses. An appropriate assessment should be undertaken in the near term and repeated periodically.
8. Future Options. The ED PIN is unlikely to serve all enterprise identification, authentication and signature needs for the future. Given the various industry and federal efforts underway to examine technologies and their appropriate business uses, FSA should avail of opportunities to participate in studies that will specifically enable its future vision.
9. Implementation. Ultimately, the enterprise-wide implementation needs to implement options that mitigate business risks. This may result in a tiered approach where more than one technology is applicable.

FSA has been communicative with all its customer groups to understand their requirements and provide innovative business solutions. Continuing this tradition of communication and partnership with customers, other Federal initiatives (e.g., E-Gov) and industry groups should also be an important part of the strategic E-Authentication business plan. Organizations focused on promoting higher education interests such as EDUCAUSE are also important partners with FSA. This type of communication is important to any implementation.

The various opportunities discussed above are summarized in the table on the following page.


OPPORTUNITIES			
	GOVERNANCE	CONTROLS	PARTNERSHIP
SHORT TERM (~ 3 - 6 Months)	<u>ARCHITECTURE</u> Develop E-ID Architecture for FSA to Standardize on Credentials Used	<u>SYSTEM REPORTS</u> Develop Management and System Reports to Identify Problems and Improve ED PIN Data Integrity	<u>RISK ASSESSMENT</u> Demonstrate ED PIN Strength, Integrity & Trust Through 3 rd Party (NIST-Based) Assessment(s)
MEDIUM TERM (~6 – 12 Months)	<u>STANDARDS</u> Develop Enterprise-Wide E-Authentication Standards & Guidance	<u>INTERNAL CONTROLS</u> Develop Internal Controls to Detect & Prevent Fraud/Identity Theft	<u>FUTURE OPTIONS</u> Learn about and Assess Other Options with Other Federal Partners: <ul style="list-style-type: none"> • PKI • Vendors & Sourcing • Trust Models • Deployment Modes
LONG TERM (~12 – 36 Months)	<u>GOVERNANCE PROCESS</u> Institute Governance Model for Architecture (how) & Standard Infrastructure (tools) for Enterprise Applications	<u>CUSTOMER STRATEGY</u> Develop Customer-Specific E-ID Strategy for Individuals and for Organizational Entities	<u>IMPLEMENTATION</u> Develop a Tiered Approach to electronic signature based on Business Risk

* * * * *


5 REFERENCES

5.1 Meeting Minutes


September 2, 2003
September 4, 2003
September 8, 2003
September 11, 2003
September 22, 2003
September 25, 2003
September 29, 2003
October 2, 2003
October 9, 2003
October 16, 2003
October 29, 2003
November 13, 2003
December 4, 2003

 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">September 2, 2003</h3>		
Attendees: 1:30 p.m. At UCP	Neil Sattler – Program Manager Yateesh Katyal – Integration Partner/ Accenture	
Purpose of Meeting	Task Order kick-off meeting.	
Decisions Made	Bi-weekly task order status report will be prepared. Task order status meeting will be weekly on Thursdays at 9:30 a.m.	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Prepare project work plan. <input checked="" type="checkbox"/> Send GFI for review (3-way CMA, OMB 300B, technical proposal for pilot, Neil's calendar for September, template for status report and project plan drafted earlier by Neil). <input type="checkbox"/> Review procedures and schedule meeting with GSA re: ED PIN credential assessment.	Yateesh Katyal Neil Sattler Yateesh Katyal
Open Action Items from Previous Meeting(s)	<ul style="list-style-type: none"> ▪ N/A. 	
Discussion	<p>The objective of the e-Authentication pilot with HHS is to demonstrate the ability of Government agencies to share credentials and develop a reusable ED PIN interface to the e-Gov gateway. It is anticipated that all federal agencies will be required to demonstrate connectivity to the gateway by FY05.</p> <ul style="list-style-type: none"> ▪ The FSA procurement to build the pilot is currently underway. A technical meeting will be scheduled with Mitretek, NSA, and others upon contract award. ▪ The 2-way credential matching agreement (CMA) between FSA/SSA is in the final stage of review. A meeting is being planned for the review. The Federal Register notice was posted on August 29, 2003. ▪ The 3-way CMA among FSA, SSA & HHS is being prepared. The FSA review is complete and changes will be discussed in a meeting with HHS and SSA. ▪ A technical meeting will be scheduled with Mitretek, NSA, and others upon contract award for the pilot. ▪ The Credential Assessment Framework (CAF) and the Password Strength document from Stephen Sill (GSA) should be reviewed. A meeting with Mr. Sill needs to be scheduled to facilitate completion of the ED PIN credential assessment. The meeting should be scheduled for UCP. 	


	<ul style="list-style-type: none"> ▪ Neil stated that an OIG audit for e-signatures is currently underway. ▪ A project work plan will be prepared. The plan should include placeholders for: <ul style="list-style-type: none"> ○ a meeting with SSA and HHS for the 3-way CMA review ○ a meeting with GSA for the credential assessment, ○ a technical meeting between GSA (gateway) and contractor (upon contract award), ○ SSIM walkthrough, and ○ ED PIN Re-Engineering walkthrough. ▪ To help comprehend the project, Neil will provide the following GFI: <ul style="list-style-type: none"> ○ OMB 300B for pilot. ○ Technical Proposal for pilot. ○ 3-way CMA. ○ Project plan drafted earlier.
<i>Next Meeting</i> 09/04/2003 9:30 a.m. UCP	<ul style="list-style-type: none"> ▪ Task Order status.

 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">September 4, 2003</h3>		
Attendees: 1:30 p.m. At UCP	Neil Sattler – Program Manager Partner/ Accenture	
	Yateesh Katyal – Integration	
Purpose of Meeting	Task Order status meeting.	
Decisions Made	N/A.	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Update / revise project work plan. <input type="checkbox"/> Obtain details re: PKI pilot with schools through NIH.	Yateesh Katyal
Open Action Items from Previous Meeting(s)	<ul style="list-style-type: none"> ▪ None. 	
Discussion	<ul style="list-style-type: none"> ▪ Discussed the need to revise and update the project plan. ▪ Question re: the percentages in the CMA – source currently unknown. Neil will check with Edith Del. ▪ The new interagency MOU in line 25 should be the 3-way CMA. Neil will work with HHS to schedule the HHS/SSA/FSA meeting to review the CMA. <ul style="list-style-type: none"> ❑ Neil talked to George Fortwengler of the Deputy Secretary's Office at HHS. He is pulling together comments on the revised draft CMA from his HRSA folks. Also, he will set up a HHS/FSA/SSA call to discuss the CMA. I told him that I would like the CMA stuff behind us by mid-September. Hopefully, our meeting initial meeting can take place next week with everything finalized by the following week. ❑ Neil also told him I was trying to pull together the technical team initial discussions also by mid-September. So if HHS drives the CMA stuff, I can drive the FSA PIN technical stuff. ▪ Schools need to be identified for participation in the pilot. ▪ The HHS business process to be used by schools during the pilot also needs to be identified. ▪ The contract award for the pilot is expected today. ▪ The credential assessment meeting with GSA has been scheduled for Monday. ▪ One of the EACs may be used as a venue to confirm pilot status in person with schools & contractors. ▪ NIH & EDUCAUSE are involved in a PKI pilot with schools. Yateesh to check about details with Peter Alterman or Mark Luker. ▪ 	


<i>Next Meeting</i> 09/08/2003 1:00 p.m. UCP	<ul style="list-style-type: none">▪ ED PIN Credential Assessment meeting with GSA.
--	--


 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">September 8, 2003</h3>		
Attendees: 1:00 p.m. At UCP	Neil Sattler – FSA Program Manager Stephen Sill, E-Authentication Applications Manager Nina Colón - ED PIN Operations Manager Yateesh Katyal – Integration Partner/ Accenture Chris Loudon & Kevin Hawkins (enspier)	
Purpose of Meeting	Initial CAF (Credential Assessment Framework) discussion as it relates to ED PIN.	
Decisions Made	N/A.	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Provide feedback to CAF team on: <ul style="list-style-type: none"> E-Authentication Common Credential Assessment Profile, and E-Authentication PIN Credential Assessment Profile <input type="checkbox"/> Schedule follow-up meeting/ develop agenda. <input type="checkbox"/> Provide specific information related to Level 2 requirements (one in “x” chance of PIN compromise).	FSA PM E-Auth AM E-Auth AM
Open Action Items from Previous Meeting(s)	<input type="checkbox"/> Update/revise project work plan.	Integration Partner
Discussion	<ul style="list-style-type: none"> Introductions. E-Authentication team provided a brief background on the CAF. The team indicated that they are following NIST guidance and developing the CAF. To-date the E-Authentication team has had preliminary discussions with USDA on WebCAAF (Web-based Central Authentication and Authorization Facility); the ED PIN discussion is the second. The intent of these discussions is to ultimately assess federal credentials for inclusion in a “Trust List” for use across the federal government through the gateway. The assessment for PIN credentials only addresses Levels 1 & 2. The requirements for assessment (CAF) are open to review and comment as part of refining the procedure. It was noted that the ED PIN is different from other PIN-based credentials in many ways: <ol style="list-style-type: none"> The ED PIN is issued on the basis of a SSA match. The ED PIN is used only in conjunction with an individual’s SSN, 	

	<p>Last Name and Date of Birth; the ED PIN is never used by itself.</p> <ol style="list-style-type: none"> 3. The ED PIN complies with GPEA and E-Sign legislation to provide electronic signature functionality. 4. The ED PIN is a randomly generated 4-digit PIN. 5. There are rules prohibiting certain easy-to-guess PINs e.g., sequential numbers. 6. The ED PIN has a history of use since 1997. <ul style="list-style-type: none"> ▪ A follow-up discussion will be scheduled for FSA comment to the framework/requirements and discussion of next steps to determine if a credential assessment for the ED PIN is applicable/beneficial. ▪ Reference Documents: <ul style="list-style-type: none"> - Entropy Rules - eAuthentication Standards for Password Strength - E-Authentication Common Credential Assessment Profile - E-Authentication Credential Assessment Framework - E-Authentication PIN Credential Assessment Profile - E-Authentication Credential Assessment Guidance - E-Authentication Password Credential Assessment Profile - E-Authentication PKI Credential Assessment Profile
Next Meeting TBD	<ul style="list-style-type: none"> ▪ Agenda - Definition of next steps.



 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">September 11 2003</h3>		
Attendees: 9:30 a.m. At UCP	Neil Sattler – FSA Program Manager Yateesh Katyal – Integration Partner/ Accenture	
Purpose of Meeting	Task Order weekly status meeting. Agenda: <ul style="list-style-type: none"> ▪ Recap from CAF Meeting ▪ Comments on CAF/PIN Profile ▪ Next Steps with CAF ▪ Project Work Plan updates ▪ Status Report – none this week ▪ Update re: PKI Pilot 	
Decisions Made	N/A.	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Draft Agenda for September 18 2003 HHS Pilot Technical Meeting. <input type="checkbox"/> Schedule Meeting with P. Alterman/M. Luker for expectation setting re: PKI pilot and HHS pilot. <input type="checkbox"/> Provide comments on CAF/CAF (PIN). <input type="checkbox"/> Update project work plan.	Y Katyal Y Katyal Y Katyal Y Katyal
Open Action Items from Previous Meeting(s)	<ul style="list-style-type: none"> ▪ Update/revise project work plan. 	Integration Partner / FSA
Discussion	<ul style="list-style-type: none"> - The technical meeting for the HHS pilot is being scheduled for September 18 1-5 pm. Likely to be a conference call. Participants will include HHS, FSA, Pearson, and Mitretek. GSA/NASA will be invited but do not see any need in attending at this stage. A draft agenda identifying the purpose and outcome of the meeting needs to be prepared. Yateesh will submit a draft to Neil for review no later than September 12 morning. The draft should cover areas such as introductions, e-Gov background, policy (CMA) update, scope of HHS pilot, participants, roles and responsibilities, expectations and timeframes, technical aspects, schools selected, etc. - FSA will determine whether the HHS pilot needs to have a PRR-like process to go live on 01/01/2004. - Yateesh has not yet heard back from Mark Luker, EDUCAUSE, re: the PKI pilot. Neil requested that a meeting be scheduled with P. Alterman, M. Luker, C. Coleman and Neil to understanding the ED role across the pilots and set expectations. 	

	<ul style="list-style-type: none">- Comments on the CAF and CAP (PIN) will be provided to Neil; the comments will address (1) feedback re: framework and profile documents, and (2) general comments.- Update the project work plan to refine known dates and activities, include a touchpoint with USDA WebCAAF project manager re: CAF, and analyze organization of work plan differently (e.g., Technology, Policy, Legal, Business, etc. activities).
<i>Next Meeting</i> 09/18/2003 9:30am 09/18/2003 1:00pm	<ul style="list-style-type: none">▪ Task Order weekly status meeting (9:30am).▪ HHS pilot Technical Meeting (1:00pm).

 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">September 22 2003</h3>		
Attendees: 9:30 a.m. At UCP	Neil Sattler – FSA Program Director Yateesh Katyal – Integration Partner/ Accenture Allen Lenis – Integration Partner/ Accenture	
Purpose of Meeting	Task Order weekly status meeting. Agenda: <ul style="list-style-type: none"> ▪ CAF Meeting Follow-up <ul style="list-style-type: none"> ○ Comments on CAF/PIN Profile ○ Next Steps with CAF ▪ Preparation for Technical Team Introductory Meeting ▪ Status Report – sent 09/15/2003. ▪ Update re: PKI Pilot 	
Decisions Made	N/A.	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Update BIG presentation and submit to Neil – complete.	A Lenis
Open Action Items from Previous Meeting(s)	N/A.	
Discussion	<ul style="list-style-type: none"> - The technical meeting for the HHS pilot will be rescheduled by Neil. The meeting earlier scheduled for September 18 1-5 pm was cancelled due to the hurricane. - Neil will provide comments on the CAF to Steve Sill and communicate next steps. - No action required on status report submitted last week. - The meeting re: the PKI pilot is scheduled for October 2 with Dr. Alterman. The meeting will be at FSA. - Neil provided comments for updating the BIG presentation. The revised package will have 5 slides that include an overview of the PMA, 5 government wide initiatives, 25 e-gov initiatives, and the pilot information. 	
Next Meeting(s) 09/18/2003 3:30pm 09/23/2003 1:00pm 09/25/2003 9:30am 10/02/2003 11:00am	<ul style="list-style-type: none"> ▪ HHS pilot Technical meeting (09/18) – to be rescheduled. ▪ FSA BIG meeting (09/23). ▪ Task Order status meeting (09/25). ▪ E-Gov meeting with Peter Alterman (10/2). 	


 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">September 25 2003</h3>		
Attendees: 9:30 a.m. At UCP	Neil Sattler – FSA Program Director Yateesh Katyal – Integration Partner/ Accenture Allen Lenis – Integration Partner/ Accenture	
Purpose of Meeting	Task Order weekly status meeting. Agenda: <ul style="list-style-type: none"> ▪ CAF Meeting Follow-up <ul style="list-style-type: none"> ○ Comments on CAF/PIN Profile ○ Next Steps with CAF ▪ Preparation for Technical Team Introductory Meeting ▪ Agenda for 10/02 PKI Pilot Meeting ▪ Next steps from FSA BIG 	
Decisions Made	N/A.	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Prepare draft agenda to be reviewed by Neil for PKI Pilot meeting – send to Neil by Friday (09/26). <input type="checkbox"/> Neil will contact Steve Sill to determine next steps for CAP/CAF. <input type="checkbox"/> Neil will reschedule Technical Team Introductory meeting (likely 09/29).	Integration Partner FSA FSA
Open Action Items from Previous Meeting(s)	<ul style="list-style-type: none"> ▪ None. 	
Discussion	<ul style="list-style-type: none"> ▪ In being proactive with the CAF/CAP team, Neil will follow up with Steve Sill to assist in the development of the Framework and Assessment Profile so that the ED PIN can be assessed at a Level 2. Neil stated that there is general support from the FSA BIG for the assessment. The next steps will likely result in a meeting. ▪ The technical team meeting for the HHS/FSA pilot is being rescheduled by Neil. Likely date is September 29. Pearson is available between 11 and 3; Neil will finalize the schedule to include Mitretek, HHS, others. ▪ Accenture will propose an agenda for the PKI pilot meeting with Dr. Alterman. The focus should be on FSA's role, information on the HHS/FSA pilot, E-Gov, Schools, etc. in addition to learning about their project. It appears that the PKI pilot team is seeking applications from the Dept. of Education that can use their solution. Neil will invite Paul Hill (or designee) to the meeting to represent the Schools channel. ▪ Neil provided an update from the BIG e-authentication presentation. The 	

	BIG was very supportive of the effort and asked to remain informed of progress.
Next Meeting(s): 09/29/2003 TBD 10/02/2003 11:00am	<ul style="list-style-type: none">▪ HHS pilot Technical meeting 09/29 TBD.▪ E-Gov meeting with Peter Alterman (10/2).


			
<div><h1>E-Authentication Pilot</h1><h2>September 29 2003</h2><h3>Meeting Minutes</h3></div>			
Attendees	<u>FSA</u> Neil Sattler Nina Colon (MitreTek) Yateesh Katyal (Accenture) Allen Lenis (Accenture) Pat Struve (Pearson) Mike Kline (Pearson) Patrick Dominy (Pearson) Eric Smith (Pearson)	<u>HHS</u> Mary Farrington Michelle Herzog	<u>GSA</u> Tice DeYoung Monette Respress
Purpose of Meeting	<p>Task Order weekly status meeting.</p> <p>Agenda:</p> <ul style="list-style-type: none">▪ Introductions (Sattler)▪ Background on E-Gov and E-Authentication (DeYoung)▪ E-Authentication Pilot (Sattler)<ul style="list-style-type: none">○ Scope (What it is & is not)○ Objectives (Which goals need to be met)○ Timelines (When)○ Key milestones (Requirements; Pilot evaluation criteria; Design; Development; Test; Deployment; Pilot evaluation; Lessons Learned)▪ Stakeholder Roles / Responsibilities (Sattler)<ul style="list-style-type: none">○ Federal Student Aid (Department of Education)○ HRSA (Department of Health & Human Services)○ U.S. General Services Administration○ Support Contractors (Pearson, Mitretek, other)○ Schools○ E-Authentication Steering Committee / E-Gov Team▪ Relationship to other pilot initiatives (Sattler)<ul style="list-style-type: none">○ Policy – CMA near complete,○ CAF/CAP assessment○ Milestones / Checkpoints▪ Next steps (All)<ul style="list-style-type: none">○ Dimensions to address (HHS business process(es), pilot school(s), architecture, issue resolution, status reports)○ Project plan inputs from stakeholders/action teams○ Meeting schedule (weekly)		

Decisions Made	Decisions to begin determining which school to use for the pilot will be held until the Pearson and Mitretek Technical teams can meet together.	
Issues/Concerns	N/A	
Open Action Items	<ol style="list-style-type: none"> 1. Need to select schools 2. Material for Requirements meetings 3. High Level Pilot Illustration 4. Next Meeting on Monday 9EST or 11:30 EST 5. ED PIN Web Services specifications 6. Mitretek Material www.cio.gov/eauthentication 	<p>Sattler/Farrington Pearson Sattler Respress</p> <p>Pearson Mitretek</p>
Open Action Items from Previous Meeting(s)	<input type="checkbox"/> None	
Discussion Items	<ul style="list-style-type: none"> ▪ Introduction – Neil Sattler introduced the participants and initiated the meeting. The objective of this pilot initiative is to have the FSA credential (ED PIN) brokered through the E-Authentication Gateway (inter-agency use of credential). ▪ Background – Tice DeYoung provided a brief background on the E-Authentication Gateway. Highlights included: <ul style="list-style-type: none"> - E-Authentication Gateway going through Certification & Accreditation - Authority to operate for 6 months and has been in operation for 3 months - The Gateway has operated without any unscheduled downtime - 3 activities supported: Gateway, Credential Providers, Credential Assessment (Framework for PIN/Passwords) ▪ E-Authentication Pilot – Neil provided an overview of the FSA/HHS E-Authentication Pilot to the participants. <ul style="list-style-type: none"> - Scope: ED PIN being extended for non-Dept of Education loan programs (Specifically, Title VII & VIII medical/nursing programs) - Objective: To enable electronic signature functionality - Timelines: All OMB Business Cases (exhibit 300) for FY05 will require interface to the E-Authentication Gateway or an explanation as to why not. Estimated schedule/milestones for the FSA/HHS E-Authentication pilot include: <ul style="list-style-type: none"> o Requirements - October 03 o Live Pilot - December 03/January 04 o Review of Pilot - February/March 04 - Key Milestones to review at conclusion of pilot: <ul style="list-style-type: none"> o Understand what it takes to go to production (steps necessary, policy discussions, testing, production planning, issue resolution, status reports, project plan inputs from 	


	<p>stakeholders/action teams, etc.)</p> <ul style="list-style-type: none"> ○ Pilot will be for limited number of schools, but involve real transactions ○ Requirements will address: date/time stamps, data collection, success/failure of authentication, etc. <ul style="list-style-type: none"> ▪ HRSA Background – May Farrington provided quick overview of pilot functions. Highlights included: <ul style="list-style-type: none"> - 22,000 Individuals participate - School customers want more electronic products similar to what they get from the Department of Education ▪ Pearson provided an overview of their task. Highlights included: <ul style="list-style-type: none"> - Support the analysis of requirements - Have a prescribed set of processes for pilot development - Will develop and manage the schedule - Pearson proposing web service and will share the documentation with team ▪ Mitretek (Monette Repress) provided an overview of proposed use of the Gateway. Highlights included: <ul style="list-style-type: none"> - User (Schools) redirection to E-authentication Gateway - Issuers of ED PIN validates status of credential - Awareness of 2 separate interfaces <ul style="list-style-type: none"> ○ Interface with FSA (for ED PIN repository) ○ Interface with applications (Schools) ○ Date & time stamps ▪ PIN API documentation to be available and distributed to needed parties (Pearson) ▪ Review (All)
Agenda for next Meeting	<ul style="list-style-type: none"> - Meeting is scheduled for Monday October 6th (9:00am ET or 11:30ET, will wait for confirmation of MitreTek Technical Staff availability, Sattler will facilitate) - Pearson and Mitretek technical teams to collaborate future Requirements and issues.
Contact	<p>Neil Sattler, Director Federal Student Aid U.S. Department of Education Neil.Sattler@ed.gov 202-377-3513</p>

 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">October 2 2003</h3>		
Attendees: 11:00a.m. At UCP	<u>FSA</u> Charlie Coleman Neil Sattler Yateesh Katyal Jesse Bowen	<u>NIH</u> Dr. Peter Alterman Keren Cummins Debbie Blanchard
	<u>EDUCAUSE</u> Mark Luker Steve Worona	
Purpose of Meeting	1. High level introduction of PKI pilot project objectives/ timelines 2. High level introduction of roles & School participation 3. Agreement on next steps.	
Agenda	<ul style="list-style-type: none"> ▪ Introductions ▪ Background on E-Gov and E-Authentication <ul style="list-style-type: none"> ○ EDUCAUSE efforts ○ NIH efforts ○ FSA efforts ▪ PKI Pilot <ul style="list-style-type: none"> ○ Scope ○ Objectives ○ Stakeholders ○ Timelines ○ Key milestones ○ Schools participation in PKI pilot ▪ Next steps. 	
Decisions Made	N/A.	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> PKI Pilot team will provide background information that includes participating schools, successes, lessons learned to FSA management. <input type="checkbox"/> HHS will provide summary description of E-Authentication ED PIN pilot with FSA to EDUCAUSE. <input type="checkbox"/> EDUCAUSE will provide suggestions to HHS for schools that should be considered for the E-Authentication ED PIN HHS pilot.	NIH FSA EDUCAUSE
Open Action Items from Previous Meeting(s)	<ul style="list-style-type: none"> ▪ N/A. 	



Discussion	<p>Charlie Coleman and Neil Sattler initiated the meeting with introductions. Key discussion points included:</p> <ul style="list-style-type: none"> ▪ NIH is directing the PKI pilot. Dr. Alterman provided a brief overview of the PKI pilot and mentioned that while he is aligned with E-Gov, his pilot is not one of the E-Gov initiatives. The PKI pilot is in operability testing. Users can download forms, sign them digitally, and upload them back to the Government. His project approach is to use a generic version of XML for the forms. The Federal Bridge Certificate Authority is part of the E-Authentication architecture even though it is not part of the Gateway. ▪ Digital Signature Trust is providing contractor support to NIH. The support includes conversion of Government forms to a generic version of XML. Form 424 was referenced as having been converted already; at a cost of about \$20,000. Current information on the NIH PKI pilot is available at www.pki.od.nih.gov. ▪ To further enhance the PKI pilot, NIH is interested in finding out which ED forms could potentially be applicable, and beneficial to FSA, for digital signatures using PKI. NIH may have funding to support the conversion of an ED form. ▪ EDUCAUSE is working with many higher education institutions. They are also supporting the PKI pilot. EDUCAUSE can send material representing relevant activities during the past 2 years. Schools participating in the PKI pilot include: <ul style="list-style-type: none"> - University of California – Berkley - University of Texas – Health Sciences Center - Dartmouth College - University of Virginia - University of Wisconsin –Madison - University of Alabama <p>EDUCAUSE will provide background information since all of the above have successfully completed the pilot with NIH. EDUCAUSE is seeking to expand the pilot to Higher Education institutions.</p> <ul style="list-style-type: none"> ▪ FSA and HHS are developing an E-Gov cross-agency pilot for electronic signature based on the ED PIN. HHS will provide an overview to EDUCAUSE re: the ED PIN pilot underway so they can assist with identifying potential schools for participation. In general, EDUCAUSE receives many requests from school customers for increased electronic transactions. ▪ FSA stated that it is important that the E-Gov teams work with other groups including the Liberty Alliance and other federal agencies to generate widely applicable functions. ▪ The meeting concluded on a positive note to share and analyze information to determine next steps.
Next Meeting TBD	<ul style="list-style-type: none"> ▪ TBD.

 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">October 9 2003</h3>		
Attendees: 9:30 a.m. At UCP	Neil Sattler – FSA Program Director Yateesh Katyal – Integration Partner/ Accenture Dana Riley - FSA	
Purpose of Meeting	Task Order weekly status meeting. Agenda: <ul style="list-style-type: none"> ▪ Feedback on 1-page FSA/HHS Pilot Summary ▪ Technical Team Schedule ▪ CAF Meeting Follow-up <ul style="list-style-type: none"> ○ Comments on CAF/PIN Profile ○ Next Steps with CAF ▪ Next Steps from NIH PKI Meeting 	
Decisions Made	Relative to the FSA/HHS pilot it is important to understand that: <ol style="list-style-type: none"> 1. FSA is responsible for developing the ED PIN electronic signature interface to the Federal Gateway. 2. HHS is responsible for making the appropriate school and business process utilize the e-sign interface. 	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Contact Mary Farrington to coordinate the pilot school selection and program information with EDUCAUSE. <input type="checkbox"/> CMA Meeting with FSA, HHS, & SSA. <input type="checkbox"/> Develop 1-page illustration of work streams. <input type="checkbox"/> Follow-up with CAP/CAF team. <input type="checkbox"/> Develop 2-page summary of NIH PKI meeting for dialogue with Schools channel. <input type="checkbox"/> Schedule meeting with Schools channel to report on NIH PKI discussion. <input type="checkbox"/> Neil will provide contact information for Mary Farrington (HHS/HRSA), Steve Sill (GSA) and George Fortwengler (HHS).	Integration Partner HHS (Fortwengler) /FSA Integration Partner FSA Integration Partner FSA FSA
Open Action Items from Previous Meeting(s)	<ul style="list-style-type: none"> ▪ None. 	

Discussion	<ul style="list-style-type: none"> ▪ The 1-page FSA/HHS pilot summary is to provide Mark Luker (EDUCAUSE) with background material, as requested. Mark's contribution to the pilot is to help identify candidate pilot schools. The summary page and request for candidate schools should therefore originate from HHS. It is the HHS business process that is being piloted; FSA is simply providing an interface to the ED PIN electronic signature function. The interface is being brokered through the Federal Gateway. Action item – Contact Mary Farrington; Neil will send contact information. ▪ For this pilot there are 3 work streams. (1) Computer Matching Agreement, (2) Technical Interface to Gateway, and (3) Credential Assessment Framework. George Fortwengler of HHS is coordinating the CMA between HHS, FSA, and SSA. The current status is that the CMA has been drafted with input from all 3 participants and George will schedule a meeting (@ SSA) for review. A current version will be forthcoming soon prior to the meeting. Action item – George will schedule meeting/send new version. ▪ It was decided to prepare a 1-page illustration of the 3 work streams that identifies the milestones and deliverables. The purpose of the illustration is to ensure all participants (including contractors) understand the goals, constraints and commitments. Suggested schedule may include 10/29 (8:30 – Noon) technical meeting between Pearson, GSA and Mitretek; 11/30 completion of development; 12/31 completion of testing/integration, etc. The milestones should be coordinated with Steve Sill as well. Overall, there are 2 E-Gov deliverables – 1. Interagency MOU by 6/30 and 2. deployment of Pilot in 2Q04. Action item – Develop 1-page work stream illustration. Yateesh will develop. ▪ Neil will follow up with the CAP/CAF team to determine next steps. ▪ It was decided that a 2-page (short) summary of the NIH PKI meeting will be prepared. The purpose of the summary will be to brief appropriate executives from the Schools channel on the dialogue with NIH as well as their request for ED Participation in the PKI pilot. Action item – Yateesh will prepare 2-page summary. Neil will schedule Schools channel meeting.
Next Meeting(s): 10/16/2003 9:30am	<ul style="list-style-type: none"> ▪ Status.

 <h2 style="text-align: center;">E-Authentication & E-Signature Support</h2> <h3 style="text-align: center;">October 16 2003</h3>		
Attendees: 9:30 a.m. At UCP	Charlie Coleman – Dy. CIO Neil Sattler – Program Director Yateesh Katyal – Integration Partner/ Accenture	
Purpose of Meeting	Task Order weekly status meeting. Agenda: <ul style="list-style-type: none"> ▪ FSA/HHS Pilot ▪ CAF Meeting Follow-up ▪ Next Steps from NIH PKI Meeting 	
Decisions Made	<ul style="list-style-type: none"> ▪ The FSA/HHS pilot will be terminated because the Federal E-Authentication Gateway is no longer available. 	
Issues/Concerns	N/A.	
Open Action Items	<input type="checkbox"/> Draft close-out action list for FSA/HHS Pilot. <input type="checkbox"/> Determine current status of Trading Partner Management credentials initiative. <input type="checkbox"/> Send executive summary for ED PIN Re-Engineering Analysis.	All Integration Partner
Open Action Items from Previous Meeting(s)	<ul style="list-style-type: none"> ▪ None. 	
Discussion	<ul style="list-style-type: none"> ▪ <u>FSA/HHS Pilot</u> The FSA/HHS pilot to use the ED PIN in an inter-agency manner is being terminated. The pilot will be terminated because the Federal E-Authentication Gateway is no longer available and is being replanned. Yateesh did have a conversation with Mary Farrington to facilitate submission of a 1-page FSA/HHS pilot summary for Mark Luker (EDUCAUSE); Mary will be contacting Neil. Actions and steps need to be determined to successfully close-out the pilot project. Action item – Develop actions for close-out. ▪ <u>CAF Meeting Follow-Up</u> IP has provided comments to FSA re: the framework. Neil was informed by GSA that another version of the framework is being released. ▪ <u>Next Steps from NIH PKI Meeting</u> A meeting with the Schools channel is required to brief them on discussion with NIH. It may be helpful to have current information on Trading Partner Management credentials. Actions – obtain current information on TPM & provide executive summary for ED PIN Re-Engineering Analysis. 	

Next Meeting(s): 10/23/2003 9:30am	<ul style="list-style-type: none">Status.
---------------------------------------	---

<div></div> <div><h1>E-Authentication</h1><h2>Discussion with FSA/HHS/GSA Pilot Team</h2><h3>October 29 2003</h3><h3>U.S. Department of Education – Office of Federal Student Aid</h3><h3>Conference Room 103B1</h3><h3>Meeting Minutes</h3></div>								
CONTACT		Neil Sattler, Director E-Commerce U.S. Department of Education Neil.Sattler@ed.gov 202-377-3513						
ATTENDEES		<table><tr><td><u>FSA</u> Charlie Coleman Neil Sattler Nina Colon</td><td><u>GSA</u> Steve Timchak</td><td><u>Accenture</u> Yateesh Katyal Jesse Bowen</td><td><u>Pearson</u> Pat Struve Mike Cline Pat Dominy</td></tr></table> <u>HHS</u> George Fortwengler Mary Farrington Michelle Herzog			<u>FSA</u> Charlie Coleman Neil Sattler Nina Colon	<u>GSA</u> Steve Timchak	<u>Accenture</u> Yateesh Katyal Jesse Bowen	<u>Pearson</u> Pat Struve Mike Cline Pat Dominy
<u>FSA</u> Charlie Coleman Neil Sattler Nina Colon	<u>GSA</u> Steve Timchak	<u>Accenture</u> Yateesh Katyal Jesse Bowen	<u>Pearson</u> Pat Struve Mike Cline Pat Dominy					
OBJECTIVES		<ol style="list-style-type: none">1. Understand current and future plans for E-Authentication initiative.2. Impact of closing current gateway on current pilot work streams.3. Possibilities for other pilot opportunities.						

AGENDA	<ul style="list-style-type: none"> • Introductions (Sattler) • Background on E-Gov and E-Authentication (Timchak) <ul style="list-style-type: none"> ◦ Progress to date ◦ GAO and TAB reports ◦ Status of gateway ◦ FSA efforts • FSA PIN Pilot Work stream Status (Sattler) <ul style="list-style-type: none"> ◦ Computer Matching Agreement ◦ Credential Assessment ◦ Pearson task order ◦ HHS schools selection ◦ Update for E-Gov reporting • New Pilot Opportunities (Timchak) <ul style="list-style-type: none"> ◦ Liberty Alliance ◦ EDUCAUSE ◦ Trading Partner Initiative ◦ STAN role • Conclusion and Next Steps (Sattler)
DECISIONS MADE	<p>GSA is preparing interim e-authentication architecture to drive future e-authentication efforts. The interim architecture will be available in the November/December timeframe. HHS will not select schools for the FSA/HHS pilot until the interim architecture is reviewed and a pilot re-defined.</p>
ISSUES/ CONCERNS	<p>It should be noted that while the Federal Gateway is closed and being re-architected, the PMA E-Gov E-Authentication effort is continuing and authentication services continue to be available through GSA.</p>
ACTION ITEMS	<ol style="list-style-type: none"> 1. FSA will complete its review of the CMA received from SSA (which includes SSA comments) and provide feedback to HHS. 2. HHS will lead the CMA review meeting with ED and SSA. OMB will be invited to facilitate. 3. GSA will provide the updated CAF documentation to ED. 4. GSA will provide the draft interim architecture to ED for distribution to appropriate participants. 5. FSA will continue its internal analysis for the ED PIN credential assessment. 6. FSA will modify the Pearson task order for scope and period of performance.
DISCUSSION ITEMS	<ul style="list-style-type: none"> ▪ Introduction – Neil Sattler initiated the meeting with introductions from all attendees.

DISCUSSION ITEMS (continued)

- **Background on E-Gov and E-Authentication** – *Steve Timchak* provided the background for the Federal Gateway which is part of the E-Authentication project under the PMA E-Gov initiatives. The centralized Federal Authentication gateway was initially affirmed by over 60 executives when it was first introduced as a concept by GSA. Standards interoperability was a paramount requirement at that time. SAML products were emerging at the time but it was decided that the gateway still needs to be developed since all of the SAML products were proprietary. On October 10 the federal gateway was “shut down” – i.e., all development activities associated with the gateway were stopped. What GSA is doing – assembling an **Architecture Working Group**. The Architecture Working Group will have an interim architecture available in the November/December timeframe. This **interim architecture** will be based on SAML interoperable products. Ensper is leading the multi-agency Architecture Working Group task force. A pilot will be demonstrated using the new architecture after it is published. Designs for the planned pilot currently include Grants.gov, National Science Foundation and U.S. Department of Agriculture. The pilot is planned to be completed by March/April of 2004 with an objective to publish an implementation guide for the interim architecture. Full operational capability for the pilot is expected by June 2004. Other items mentioned by Steve include:
An **E-Authentication PMO** will help become a clearinghouse for products that are interoperable using the GSA laboratory.
Policy activities are still ongoing and include work related to the assurance levels.
The **Federal Bridge** is available for cross-certifying domains. The E-Authentication initiative is also developing a **Credential Assessment Framework** (CAF) for PIN and Password (in addition to PKI) solutions.
The first **credential assessment** (conducted by ORC) has been completed for Grants.gov.
The **Federal Identity Credentialing Committee** is also seeking to standardize credentials for Government personnel.
- **ED PIN Pilot Work stream Status** –
- **Computer Matching Agreement** – The computer matching agreement draft is evolving to allow use of the ED PIN outside of Title IV programs. SSA has provided comments to ED on the current draft. ED will provide the next draft to HHS⁵. HHS will schedule a 3-way meeting to ensure SSA, ED and HHS are all agreeable to the computer matching agreement⁶. OMB may be invited to attend the 3-way meeting to facilitate issue resolution. *Steve* is not aware of any other agency pursuing this type of agreement.
- **Credential Assessment** – FSA will continue activities associated with

⁵ Action item #1.

⁶ Action item #2.

DISCUSSION ITEMS (continued)

the credential assessment for the ED PIN. GSA is updating the CAF documentation and will provide a current draft to FSA⁷. GSA will also provide a copy of the interim architecture in its draft form to Neil for distribution to participants⁸. FSA will review the documentation for the CAF and the architecture in preparation for a credential assessment⁹. While no date has been scheduled for a credential assessment of the ED PIN, FSA expects it to be within the next few months. GSA indicated that the actual assessment usually takes a couple of days and assessors will be willing to visit the Pearson data center/facilities associated with the ED PIN.



- **Pearson Task Order** – The Pearson task order in support of the FSA/HHS pilot will be modified in scope, if necessary¹⁰. Pearson will support the assessment and prepare appropriate plans for the assessment. The period of performance for the Pearson task order should be extended and a SAML focus is added as part of the task order modification. Per *Steve Timchak*, the point of contact for the CAF is *Steve Sill*.
- **HHS School Selection** – A little more planning needs to be performed before schools are selected by HHS. HHS will wait until the interim architecture and the pilot is defined so that appropriate schools can be contacted. No action for school selection is required at this time. The current actions for the CMA will continue and next steps related to the pilot will be evaluated mid-January.
- **Update for E-Gov Reporting** – GSA, HHS and ED concur on the activities previously planned for the FSA/HHS pilot. The planned deliverables are no longer required. However, E-Gov E-Authentication support is continuing and activities being redefined.
- **New Pilot Opportunities** – New pilot opportunities will be identified collaboratively immediately following the publication of the interim architecture by GSA.
- **Conclusions and Next Steps** – *Neil Sattler* provided a summary of the meeting. The meeting concluded successfully and action items will be communicated to the respective participants.

⁷ Action item #3.

⁸ Action item #4.



⁹ Action item #5.

¹⁰ Action item #6.

  <h2 style="text-align: center;">E-Authentication Pilot</h2> <h3 style="text-align: center;">November 13, 2003</h3> <h3 style="text-align: center;">Meeting Minutes</h3>		
Attendees	Neil Sattler Yateesh Katyal (Accenture) Jesse Bowen (Accenture)	
Purpose of Meeting	Task Order weekly status meeting. Agenda: <ul style="list-style-type: none"> ▪ Interim Architecture ▪ CAF Follow-Up ▪ Risk Assessment ▪ Additional Focus 	
Decisions Made	The task order deliverables need to be modified since the E-Authentication Gateway and the FSA-HHS pilot have been put on hold for the time being.	
Issues/Concerns	<ol style="list-style-type: none"> 1. The Credential Assessment Framework in development by the GSA E-Authentication team does not include guidance for knowledge-based authentication. This is an issue because without that guidance, the ED PIN will be treated as any other PIN credential thereby reducing the ED PIN superiority and assurance level. 2. NIST Special Publication 800-63, DRAFT Recommendation for Electronic Authentication, does not include any guidance for knowledge-based authentication. This is a concern because the guidance is not directly beneficial for the ED PIN credential. 3. Potential issue: A decision should be made as to which framework the ED PIN will be assessed against – the GSA CAF or the NIST Special Publication 800-63. At the moment, the 2 appear to be covering the same scope and competing against each other. 	
Open Action Items	7. Revise Task Order 144.	Accenture/FSA
Open Action Items from Previous Meeting(s)	<input type="checkbox"/> N/A.	
Discussion Items	The meeting focused on next steps to facilitate FSA's participation and contribution towards E-Gov E-Authentication efforts. There are 3 activities that are currently required:	

	<ol style="list-style-type: none"> 1. <u>White Paper support.</u> It is anticipated that a white paper outlining steps FSA should take to continue its progress with E-Authentication will be developed. The specific content to be addressed has not yet been decided. This white paper can be the pre-cursor for a potential business case to either participate in a pilot with another organization or to fund a FSA pilot. 2. <u>Assessment.</u> It is likely that FSA will utilize Accenture support during the planned ED PIN credential assessment. This assessment is in association with the Credential Assessment Framework in development by the GSA E-Authentication team. 3. <u>Comments on, and review of, emerging documents.</u> To date, the following documents have been recently developed by associated organizations: <ol style="list-style-type: none"> a. Credential Assessment Framework (GSA E-Gov E-authentication) b. Interim Architecture (GSA E-Gov E-Authentication) c. DRAFT Recommendation for Electronic Authentication, NIST Special Publication 800-63 (NIST). d. SAML Artifact Profile as an Adopted Scheme for E-Authentication, Draft Version 0.0.1 (GSA E-Gov E-Authentication) e. E-Authentication Interface Specifications for the SAML Artifact Profile, Draft Version 0.1.0 (GSA E-Gov E-Authentication) f. Technical Approach for the E-Authentication Interim Capability, Draft Version 0.0.1 (GSA E-Gov E-Authentication). 4. <u>NIH PKI Pilot.</u> EDUCAUSE and NIH are supporting a pilot with higher education institutions to determine if the use of PKI and associated credentials are beneficial. <p>The scope of the current task order needs to be revised. The revision will be proposed within the next 4 weeks by Accenture. The revision will be based on the current funding level to determine scope.</p> <p><u>High Level Review Comments – NIST Special Publication 800-63, DRAFT Recommendation for Electronic Authentication.</u></p> <p>The draft addresses several factors related to authentication of individual people over an open network: the registration process (claimant, verifier, establishing an identity, and relying parties), tokens (e.g., password, cryptographic key, smart card, voice print, biometrics), verifiers and assertions (e.g., SAML, cookies, etc.). The draft also illustrates how electronic authentication can vary relative to the strength of a credential itself (i.e., difficulty of guessing, forging, or otherwise compromising a credential) and discusses the potential use of entropy to determine requisite strength of a credential/password.</p> <p>The ED PIN as an authentication credential. It is not simply a PIN password or PIN number. The ED PIN credential is the US Department of Education, FSA name for the credential that includes a person's social security number, date of birth, first two letters of the last name, and a 4-digit password. The first three components of the ED PIN credential are knowledge-based aspects related to an individual. The paper does not</p>
--	--

	<p>consider knowledge-based authentication methods. The draft indicates that guidance for knowledge-based authentication will be made available but no timeframe is provided. The analysis of knowledge-based authentication using other models would not do proper justice to the ED PIN credential strength.</p> <p>The current ED PIN possesses important controls that need to be recognized. For example: SSL/TLS protects the channel and prevents eavesdropping; the ED PIN is encrypted during storage; accounts are locked after a specified number of incorrect login attempts, which increases the difficulty of guessing the credential. There are other controls as well.</p> <p><u>One suggestion</u> would be for FSA to partner with NIST, and/or GSA (as appropriate), to help develop the knowledge-based authentication framework. Other federal agencies interested in this framework may also be included in this effort.</p>		
Agenda for next Meeting	<p>December 4 2003 TBD</p>		
Contact	<table> <tr> <td> Neil Sattler, Director Federal Student Aid U.S. Department of Education Neil.Sattler@ed.gov Yateesh.Katyal@Accenture.com 202-377-3513 </td> <td> Yateesh Katyal, Ph.D. Integration Partner Accenture 703-947-3510 </td> </tr> </table>	Neil Sattler, Director Federal Student Aid U.S. Department of Education Neil.Sattler@ed.gov Yateesh.Katyal@Accenture.com 202-377-3513	Yateesh Katyal, Ph.D. Integration Partner Accenture 703-947-3510
Neil Sattler, Director Federal Student Aid U.S. Department of Education Neil.Sattler@ed.gov Yateesh.Katyal@Accenture.com 202-377-3513	Yateesh Katyal, Ph.D. Integration Partner Accenture 703-947-3510		

  <h2 style="text-align: center;">E-Authentication Pilot</h2> <h3 style="text-align: center;">December 4, 2003 Meeting Minutes</h3>		
Attendees	Charlie Coleman Neil Sattler Harry Feely (Follow-On meeting subsequent to TO Status) Yateesh Katyal (Accenture)	
Purpose of Meeting	Task Order weekly status meeting. Agenda: <ul style="list-style-type: none"> ▪ Comments on E-Authentication Draft Strategic Business Plan ▪ High level Task Order work plan 	
Decisions Made	N/A.	
Issues/Concerns	N/A. See discussion items below.	
Open Action Items	8. Revise Task Order 144. Request received from FSA.	In process - Accenture/FSA
Open Action Items from Previous Meeting(s)	<input type="checkbox"/> N/A.	
Discussion Items	<p>The document titled “Draft Strategic Plan Comments.doc” captured the issues and concerns with the Draft Strategic Business Plan. The comments were discussed with FSA and forwarded to Harry Feely for communication to GSA. The comments are being provided at GSA’s request. FSA also provided a suggestion for drivers associated with the business plan in graphic form.</p> <p>A high level project work plan for the revised Task Order 144 was also discussed. This 1-page work plan will be reviewed by Neil and updated accordingly.</p>	
Agenda for next Meeting	December 11, 2003 TBD	

Contact	Neil Sattler, Director Federal Student Aid U.S. Department of Education Neil.Sattler@ed.gov Yateesh.Katyal@Accenture.com 202-377-3513	Yateesh Katyal, Ph.D. Integration Partner Accenture 703-947-3510
----------------	---	---

5.2 FSA-HHS E-Sign (E-Gov E-Authentication) Pilot Description

The U.S. Department of Education Federal Student Aid (FSA) CIO Office of Applications Development supports the President's Management Agenda through multiple government-wide E-Gov efforts. For electronic authentication (E-Authentication), FSA is continuing its effort to promote customer use of electronic signatures in the student, school and financial partner communities. Specifically for E-Authentication, FSA is piloting the development of a solution that leverages the Federal E-Authentication Gateway to provide electronic signature (E-Sign) capability across multiple federal agencies.

FSA desires to use electronic identities issued to our customers as a means to replace traditional paper-based transactions and business processes; and, to use these electronic identities in conjunction with E-Gov E-Authentication initiatives, as appropriate. FSA has successfully established an E-Sign capability available to its own users and customers and has successfully implemented the E-Sign capability for promissory notes in the Direct Loan, FFEL, and Perkins programs, as well as the Free Application for Federal Student Aid (FAFSA). The E-Sign capability provides an additional level of customer service and meets the legislative mandates of the E-SIGN Act and GPEA. FSA's most recent E-Authentication effort is to pilot the E-Sign capability across multiple federal agencies using the FSA student credential. This student credential – the ED PIN – is issued to nearly 8 million students each year by FSA and has been successfully used to electronically sign over a million documents. The issuance of an ED PIN credential to individuals conforms to strict processes for identity validation that include matching data with the U.S. Social Security Administration (SSA).

FSA is leading a pilot initiative with HHS to share the ED PIN electronic credential for student financial aid applicants and borrowers – in this case, across federal agencies. The provision of electronic means of conducting business, as an alternative to paper-based processes, can potentially reduce unit cost for federal agencies and schools while increasing customer satisfaction. Use of the already implemented Federal E-Authentication Gateway as a service to broker the transaction minimizes investment for cross-agency use of E-Sign functionality. The objective of the pilot is to document all the necessary activities for a production-ready E-Sign capability based on the ED PIN for use across Government agencies. The pilot effort is currently underway and is anticipated to be completed in March 2004.



October 6, 2003



Contact Information:
Neil Sattler, Director
Federal Student Aid
U.S. Department of Education
Neil.Sattler@ed.gov
202-377-3513